IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **French et al.**	§	
	§	Confirmation No.: **1697**
Serial No. **09/930,328**	§	
	§	Group Art Unit: **2137**
Filed: **August 15, 2001**	§	
	§	Examiner: **Popham, Jeffrey D.**
For: **Method and System for Managing Resources Using Geographic Location Information Within a Network Management Framework**	§	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

35525
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on November 14, 2007.

A fee of $510.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees, which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation of Armonk, New York.

RELATED APPEALS AND INTERFERENCES

This appeal has no related appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

The claims in the application are: 1-40

B. STATUS OF ALL THE CLAIMS IN APPLICATION

Claims canceled: None

Claims withdrawn from consideration but not canceled: 15-17, 32-34, and 38-40

Claims pending: 1-14, 18-31, and 35-37

Claims allowed: None

Claims rejected: None

Claims objected to: None

C. CLAIMS ON APPEAL

The claims on appeal are: 1-14, 18-31, and 35-37

STATUS OF AMENDMENTS

A Response after the Final Office Action was not filed.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIM 1 – INDEPENDENT

The subject matter of claim 1 is directed to a method for management of a distributed data processing system. A unique network hardware identifier for a network device is determined (Specification, page 26, line 15 – page 27. line 4; page 82, lines 20-28; page 83, line 24 – page 87, line 17; Figure 18, 1814; Figure 19A and 19B). The unique network hardware identifier is associated with geographic location information (Specification, page 81, lines 4-25; page 83, line 24 – page 87, line 17; Figure 18, 1806 Figure 19A and 19B). The network device is configured in accordance with the geographic location information through a network administrative user interface (page 28 lines 7-32; page 29, lines 18-25; 91, line 7 – page 92, line 30; Figure 5).

B. CLAIM 18 – INDEPENDENT

The subject matter of claim 18 is directed to an apparatus for management of a distributed data processing system. The apparatus comprises a means for determining unique network hardware identifier for a network device (Specification, page 26, line 15 – page 27. line 4; page 82, lines 20-28; page 83, line 24 – page 87, line 17; Figure 18, 1814; Figure 19A and 19B); a means for associating the unique network hardware identifier with geographic location information (Specification, page 81, lines 4-25; page 83, line 24 – page 87, line 17; Figure 18, 1806 Figure 19A and 19B); and a means for configuring the network device in accordance with the geographic location information through a network administrative user interface (page 28 lines 7-32; page 29, lines 18-25; 91, line 7 – page 92, line 30; Figure 5).

C. CLAIM 35 – INDEPENDENT

The subject matter of claim 35 is directed to computer program product in a computer readable medium for use in managing a distributed data processing system. The computer program product comprises: instructions for determining a unique network hardware identifier for a network device (Specification, page 26, line 15 – page 27. line 4; page 82, lines 20-28; page 83, line 24 – page 87, line 17; Figure 18, 1814; Figure 19A and 19B); instructions for associating the unique network hardware identifier with geographic location information (Specification, page 81, lines 4-25; page 83, line 24 – page 87, line 17; Figure 18, 1806 Figure 19A and 19B); and instructions for

configuring the network device in accordance with the geographic location information through a network administrative user interface (page 28 lines 7-32; page 29, lines 18-25; 91, line 7 – page 92, line 30; Figure 5).

D. CLAIM 4 – DEPENDENT

The subject matter of claim 4 is directed to the method of claim 1 further comprising generating a unique name for an endpoint resource on the network device, wherein the unique name comprises the geographic location information (page 82, line 16-19; page 84, line 32 – page 85, line 12; page 86, lines 2-32; page 87, lines 14-18; Figure 18, 1812; Figure 19A and 19B, 1910, 1912, 1914, 1916, 1918, 1926, 1942, and 1948).

E. CLAIM 21 – DEPENDENT

The subject matter of claim 21 is directed to the apparatus of claim 18, further comprising a means for generating a unique name for an endpoint resource on the network device, wherein the unique name comprises the geographic location information (page 82, line 16-19; page 84, line 32 – page 85, line 12; page 86, lines 2-32; page 87, lines 14-18; Figure 18, 1812; Figure 19A and 19B, 1910, 1912, 1914, 1916, 1918, 1926, 1942, and 1948).

F. CLAIM 5 – DEPENDENT

The subject matter of claim 5 is directed to the method of claim 4, further comprising associating the unique name with security attributes for the endpoint resource (page 82, line 10-13; page 87 line 24 – page 88, line 15; Figure 18, 1810; Figure 20).

G. CLAIM 22 – DEPENDENT

The subject matter of claim 22 is directed to the apparatus of claim 21, further comprising means for associating the unique name with security attributes for the endpoint resource (page 82, line 10-13; page 87 line 24 – page 88, line 15; Figure 18, 1810; Figure 20).

H. CLAIM 6 – DEPENDENT

The subject matter of claim 6 is directed to the method of claim 4, further comprising associating the unique name for the endpoint resource with the unique network hardware identifier (page

82, line 29- page 83, line 7 page 84, line 32 – page 85, line 12; page 86, lines 2-32; page 87, lines 14-18; Figure 18, 1816; Figure 19A and 19B, 1910, 1912, 1914, 1916, 1918, 1926, 1942, and 1948).

I. CLAIM 23 – DEPENDENT

The subject matter of claim 23 is directed to the apparatus of claim 21, further comprising means for associating the unique name for the endpoint resource with the unique network hardware identifier (page 82, line 29- page 83, line 7 page 84, line 32 – page 85, line 12; page 86, lines 2-32; page 87, lines 14-18; Figure 18, 1816; Figure 19A and 19B, 1910, 1912, 1914, 1916, 1918, 1926, 1942, and 1948).

J. CLAIM 10 – DEPENDENT

The subject matter of claim 10 is directed to the method of claim 1 further comprising detecting a change of location of the network device within the distributed data processing system based on the geographic location information (page 88, line 16 - page 90, line 2; Figure 21).

K. CLAIM 27 – DEPENDENT

The subject matter of claim 27 is directed to the apparatus of claim 18, further comprising means for detecting a change of location of the network device within the distributed data processing system based on the geographic location information (page 88, line 16 - page 90, line 2; Figure 21).

L. CLAIM 11 – DEPENDENT

The subject matter of claim 11 is directed to the method of claim 10 further comprising reconfiguring the network device based on the detected change of location of the network device (page 88, line 16 - page 90, line 2; page 102, lines 6-14; Figure 21).

M. CLAIM 28 – DEPENDENT

The subject matter of claim 28 is directed to the apparatus of claim 27, further comprising means for reconfiguring the network device based on the detected change of location of the network device (page 88, line 16 - page 90, line 2; page 102, lines 6-14; Figure 21).

N. CLAIM 12 – DEPENDENT

The subject matter of claim 12 is directed to the method of claim 10 further comprising reconfiguring user security parameters based on the detected change of location of the network device. (page 87; line 24 – page 88, line 15; page 88, line 16 - page 90, line 2; page 102, lines 6-14;Figure 20, figure 21).

O. CLAIM 29 – DEPENDENT

The subject matter of claim 29 is directed to the apparatus of claim 27, further comprising means for reconfiguring user security parameters based on the detected change of location of the network device. (page 87; line 24 – page 88, line 15; page 88, line 16 - page 90, line 2; page 102, lines 6-14;Figure 20, figure 21).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection to review on appeal are as follows:

A. GROUND OF REJECTION 1

Whether the Examiner has stated a *prima facie* obviousness rejection under 35 U.S.C. § 103 against claims 1-14, 18-31, and 35-37 based on *Liming et al,* System and Method Providing a Spatial Location Context, U.S. Patent Application Publication 2002/0055924, May 9, 2002 (hereinafter "*Liming*") in view of *Hougaard et al.*, Geographic-Based Information Technology Management System, U.S. Patent No. 6,216,130, April 10, 2001 (hereinafter "*Hougaard").*

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1-14, 18-31, and 35-37)

The Final Office Action rejects claims 1-14, 18-31, and 35-37 under 35 U.S.C. § 103 as being unpatentable over *Liming et al,* System and Method Providing a Spatial Location Context, U.S. Patent Application Publication 2002/0055924, May 9, 2002 (hereinafter "*Liming*") in view of *Hougaard et al.*, Geographic-Based Information Technology Management System, U.S. Patent No. 6,216,130, April 10, 2001 (hereinafter "*Hougaard*").

A.1. *Claims* 1-14, 18-31, and 35-37

Regarding Claim 1, the Final Office Action States:

> Liming discloses a method for management of a distributed data processing system, the method comprising:
>
> Determining a unique network hardware identifier for a network device (Paragraphs 73-74; 99-100; and 156-159);
>
> Associating the unique network hardware identifier with geographic location information (Paragraphs 73-74; 99-100; and 156-159); and
>
> Managing the network in accordance with the geographic location information (Paragraphs 156-162);
>
> But does not explicitly disclose configuring the network device in accordance with the geographic location information through a network administrative user interface.
>
> Hougaard, however, configuring the network device in accordance with the geographic location information through a network administrative user interface (Column 5; line 32 to Column 6, line 19; and Column 7, lines 1-62). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the geographic-based management system of Hougaard into the location-based network system of *Liming* in order to allow the system of organize geographic information located at remote sources in such a way that it is easily accessible and displayable to users, facilitate the exchange and distribution of geographic information to multiple users within an organization, and/or to allow an administrator to specify which users are authorized to access, modify, or delete geographic information through filters.

Final Office Action dated September 26, 2007, pp. 3-4.

Independent claim 1, which is representative of claims 18 and 35, is as follows:

> 1. A method for management of a distributed data processing system, the method comprising:
>
> determining a unique network hardware identifier for a network device;
>
> associating the unique network hardware identifier with geographic location information; and
>
> configuring the network device in accordance with the geographic location information through a network administrative user interface.

No *prima facie* obviousness rejection of claim 1 can be stated in view of *Liming* and *Hougaard* because neither *Liming* nor *Hougaard*, either alone or in combination, teaches the features of claim 1. The Examiner bears the burden of establishing a *prima facie* case of obviousness based on prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). The scope and content of the prior art are... determined; differences between the prior art and the claims at issue are... ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or non-obviousness of the subject matter is determined. *Graham v. John Deere Co.*, 383 U.S. 1 (1966). Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue. *KSR Int'l. Co. v. Teleflex, Inc.*, No. 04-1350 (U.S. Apr. 30, 2007). Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *Id.* (citing *In re Kahn*, 441 F.3d 977, 988 (CA Fed. 2006)).

A *prima facie* obviousness rejection cannot be stated because the proposed combination of the references does not teach or suggest all the features of claim 1. Specifically, neither *Liming* nor *Hougaard*, either alone or in combination, teaches or suggests the feature of **configuring the network device in accordance with the geographic location information through a network administrative user interface**. The Final Office Action admits that *Liming* does not teach this feature. (See Final Office Action dated September 26, 2007, p. 4.) However, the Final Office Action points to *Hougaard*, column 5, line 32 to column 6, line 19, and column 7, lines 1-62, which are reproduced below for the Board's convenience, as allegedly teaching this feature:

> FIG. 1 provides an overview of the architecture of one embodiment of the systems of the invention. In this embodiment, the system includes an administrator application 10 whereby an administrator organizes information referencing geographic and other data structures available at remote data sources. The user application 20 accesses the reference information generated by administrator application 10 and retrieves and displays the geographic and other data structures located at the remote sources.
>
> Administrator application 10 is executed at a administrator system 11, while user application 20 is executed at a user system 21. Administrator system 11 and user system 21 may each be a separate computer or computer system. For example, administrator system 11 may be embodied in a server computer, while user system 21 may be embodied in a client computer in a network environment. In this configuration, multiple

users may have access to the information compiled by administrator application 10 using a plurality of user applications 20, each installed on a separate client computer. Alternatively, administrator system 11 and user system 21 can be embodied in a single computer. The invention extends to systems wherein administrator application 10 and user application 20 are program modules of a single application program executed on one computer.

As shown in FIG. 1, the systems of the invention enhance the usability and accessibility of disorganized data sources 30, which may be located anywhere in the world. A GIS administrator uses administrator application 10 to identify, from disorganized data sources 30, the information that is of interest to individuals within the organization that is to be served by the systems of the invention. For example, the administrator may browse or otherwise search the Internet via network infrastructure 44. The disorganized data sources 30 may include geographic data 12, tabular data 14, application programs 16, and other data 18, such as graphical images, video, and audio. Depending on the interests of users within the organization, the administrator may choose to identify any number or type of data structures from disorganized data sources 30.

In one example, the organization to be served by the system of FIG. 1 may be a public utility. In this case, the geographic data 12 may represent maps of the region served by the public utility, including municipal boundaries, streets, and information relating to the physical infrastructure of the public utility. Tabular data 14 may include customer lists, while applications 16 may be software for displaying the geographic data and tabular data to users. Other data 18 may be any type of information that further pertains to the infrastructure or services provided by the public utility. Of course, the system of FIG. 1 may instead be used by essentially any other type of organization, and the data structures at the disorganized data sources 30 may be any type of data deemed to be of importance to the particular organization.

Hougaard, column 5, line 32 to column 6, line 19.

By compiling data references 22, the administrator establishes an index of useable data structures located at disorganized data sources 30 and makes the index available to any desired number of users in the organization. Referring again to the example of a public utility, the administrator can organize data references 22 to allow customer service representatives, maintenance dispatchers, and other interested users to conveniently retrieve and view the geographic information likely to be of importance to the public utility. In the absence of data references 22 and other information stored by administrator application 10, individual users in the organization would be required to locate and organize the geographic data 12 and other data structures, thereby engaging in inefficient duplication of effort.

In addition to merely locating referencing data structures 12, 14, 16, and 18, the administrator application 10 allows an administrator to establish relationships between various data structures or combinations of data structures. To illustrate the concept of establishing relationships between data structures, an administrator in a public utility may identify three data structures. A first geographic data structure may include an encoded map of the streets, municipal boundaries, and other features of a portion of the

geographic region of service of the public utility. A second geographic data structure may include, for example, a representation of the infrastructure of the public utility. A tabular data structure may list customers of the public utility along with the customers' addresses. The administrator, in this example, decides that users within the public utility would be interested in viewing a map wherein the images of the two geographic data structures are combined. Moreover, the administrator may determine that users in the public utility would be interested in viewing or otherwise using the tabular customer data when viewing the map associated with the two geographic data structures.

In order to facilitate the combined use of the two geographic data structures and the tabular data structure, the administrator can specify the relationship between the data structures in relationship information 32. A detailed description of one technique for organizing and establishing relationships between data structures is presented below in reference to FIG. 2.

Referring to FIG. 1, the administrator application 10 also compiles other information that allows users to access the appropriate data indexed by data references 22. The administrator can configure context filters 34, which permits the users to receive only the geographic and other data that is relevant to them a that time that the requests for data are made. The administrator can also configure user access filters 36, which constitute a security mechanism for allowing only authorized users to access the geographic and other data. The administrator can compile application specific data 38, which specify application specific paths or mode information required to display tabular data or other types of data. The application specific data 38 allow tabular and other data to be conveniently displayed to the user without the user having to manually specify the application specific paths or mode information. In summary, the information compiled by the administrator using administrator application 10 organizes data structures 12, 14, 16, and 18 located at disorganized data sources 30 in a manner to make them accessible to users of the system of FIG. 1.

Hougaard, column 7, lines 1-62.

The passage of *Hougaard* in column 5, line 32 to column 6, line 19, does not teach the feature of **configuring the network device in accordance with the geographic location information through a network administrative user interface.** Rather, the column 5, line 32 to column 6, line 19 passage of *Hougaard* teaches organizing geographic data gathered from disparate sources.

The passage of *Hougaard* in column 7, lines 1-62, also fails to teach the feature of **configuring the network device in accordance with the geographic location information through a network administrative user interface.** Rather, the passage of *Hougaard* in column 7, lines 1-62 teaches that an administrator can compile data and establish an index of useable data structures located at disorganized locations. This information is then made available to the users. Additionally, the administrator can establish relationships between various data structures or combinations of data structures. As stated in

column 7, lines 58-62, "In summary, the information compiled by the administrator using administrator application **10** organizes data structures **12**, **14**, **16**, and **18** located at disorganized data sources **30** in a manner to make them accessible to the users of the system in FIG. 1." (emphasis added)

In the Final Office Action, mailed September 26, 2007, the Examiner points specifically to lines 45-52 of the above-cited column 7, lines 1-62, as teaching this feature. Lines 45-62 of column 7 of *Hougaard* state, "The administrator can configure context filters 34, which permits the users to receive only the geographic and other data that is relevant to the user at the time that the requests for data are made. The administrator can also configure user access filters 36, which constitute a security mechanism for allowing only authorized users to access the geographic and other data." Appellants submit that this passage merely teaches that users are allowed access only to specific geographic data rather than all geographic data. This passage does not teach or suggest anything regarding **configuring the network device in accordance with the geographic location information through a network administrative user interface.**

The passage of lines 45-62 of column 7 of *Hougaard* describes Figure 1. When looking at Figure 1, one can clearly see that the context filters referred to are part of an administrator application located in an administrator system. This administrator application is in communication with a user application that is located on a user system. The context filters do not configure either the user system or the administrator system. The administrator system is not altered or configured **in accordance with the geographic location information,** as the location of the administrator system has nothing to do with access to the data or the way in which the system operates. Rather, all the data still resides in the administrator system and is accessible by various users regardless of the location of the administrator system. Additional, the user system also is not altered or configured **in accordance with the geographic location information**.

The context filters do not cause anything to happen to the user system. That is, the user system is not configured **in accordance with the geographic location information.** Rather, the user system is simply allowed access to certain geographic information. Column 8, lines 15-18 states that users access may be based on authorization parameters associated with the user. However, the authorization parameters are not defined or explained. However, *Hougaard* uses a public utility as an example and explains how a public utility worker is allowed access to certain types of data, such as maps of the region served by the public utility, including municipal boundaries and streets. (See *Hougaard*, Column 6, lines 5-10). Thus, the location of the user or user system is also irrelevant to the geographic and other data obtained by the user.

Hougaard teaches limiting access to users to specific types of geographic information that are deemed relevant or appropriate for that user. However, *Hougaard* does not teach configuring a network device in accordance with the geographic location information. In contradistinction, claim 1 recites **configuring the network device in accordance with the geographic location information through a network administrative user interface.** Several examples of configuring a network in accordance with the geographic location information are discussed in the specification. For example, a user may be granted access based to a network or portions of a network based on the geographic location of the user. That is, a user in one region may be granted access to only a portion of a network because of the geographic area the device is located in when the device accesses the network.

Another example of configuring a network device in accordance with the geographic location information through a network administrative user interface includes the distribution of software to devices within the network based upon the geographic information associated with each device. For example, devices within some networks may require software that is specifically configured for a device depending on its geographic location. For example, an ISP may be required to provide certain functionality within a given geographic region.

As another example, a user may desire to update all the data processing systems within a network with the newest revision of certain software packages. However, the newest revision of a software application may comprise multiple versions that are individually configured for different geographic regions. For instance, a corporate customer may desire that the accounting departments throughout an enterprise have the latest revision of a software application that computes taxes in accordance with the tax laws of a given geographic region, which might require special software modules, tax forms, etc., for each geographic region.

The passage of *Hougaard* in column 5, line 32 to column 6, line 19 merely teaches organizing data for the easy use and retrieval by a user. However, the passage does not teach **configuring the network device in accordance with the geographic location information through a network administrative user interface.** In fact, the passage of *Hougaard* in column 5, line 32 to column 6, line 19 makes no mention of configuring either a network or network devices. Accordingly, the passage of *Hougaard* in column 5, line 32 to column 6, line 19, fails to teach or suggest the feature of **configuring the network device in accordance with the geographic location information through a network administrative user interface.**

The passage of *Hougaard* in column 7, lines 1-62, also fails to teach the feature of **configuring the network device in accordance with the geographic location information through a network administrative user interface.** Rather, the passage of *Hougaard* in column 7, lines 1-62 teaches that an

administrator can compile data and establish an index of useable data structures located at disorganized locations. Therefore, the passage of *Hougaard* in column 7, lines 1-62, fails to teach the feature of **configuring the network device in accordance with the geographic location information through a network administrative user interface.** Furthermore, the passage of *Hougaard* in column 7, lines 1-62 does not mention configuring either a network or network devices. Accordingly, the passage of *Hougaard* in column 7, lines 1-62 fails to suggest the feature of **configuring the network device in accordance with the geographic location information through a network administrative user interface.**

As stated in column 4, lines 38 through 40 of *Hougaard*, the invention taught by *Hougaard* is directed to managing, organizing and retrieving geographic and other data. No portion of *Hougaard* addresses, talks about, or even hints at configuring a network or network devices, or **configuring the network device in accordance with the geographic location information through a network administrative user interface.** Therefore, *Hougaard* fails to teach or suggest the feature of **configuring the network device in accordance with the geographic location information through a network administrative user interface.**

For at least the reasons set forth above, *Hougaard* fails to solve the deficiencies of *Liming* in regards to claim 1. Therefore, the proposed combination of *Liming* and *Hougaard*, when considered as a whole, does not teach or suggest all of the features of claim 1. For this reason, the proposed combination of *Liming* in view of *Hougaard* fails to render obvious claim 1. Furthermore, as claim 1 is representative of claims 18 and 35, the distinctions between claim 1 and the proposed combination of *Liming* in view of *Hougaard* apply to claims 18 and 35. Therefore, the proposed combination of *Liming* in view of *Hougaard* fails to render obvious claims 18 and 35. Additionally, claims 2-14, 19-31, 36, and 37 depend from claims 1, 18, and 35. Accordingly, no *prima facie* obviousness rejection can be stated against claims 1-14, 18-31, and 35-37. Therefore, Appellants respectfully request that the rejection of claims 1-14, 18-31, and 35-37 under 35 U.S.C. § 103 be reversed.

A.1.a Claims 4 and 21

Additionally, claims 2-14, 19-31, 36, and 37 disclose other features not taught or suggested by the combination of *Liming* in view of *Hougaard*. For example, claims 4-6, 10-12, 21-23, and 27-29 all recite features that are not taught or suggested by the combination of *Liming* in view of *Hougaard*.

Claims 4 and 21 recite the feature of "generating a unique name for an endpoint resource on the network device, wherein the unique name comprises the geographic location information." The

Examiner cites to *Liming*, paragraphs 88-90, 107-110, and 160-165 as teaching this feature. However, none of these passages teaches the feature of "generating a unique name for an endpoint resource on the network device, wherein the unique name comprises the geographic location information."

Paragraphs [0088] – [0090] of *Liming* teach storing location information in a database. The database may include entries for the IP address of the device or system, location descriptors, time the location is determined, time the information is received and/or recorded, and the method by which the location descriptor was determined. Nowhere does this passage teach or suggest the feature of "generating a unique name for an endpoint resource on the network device, wherein the unique name comprises the geographic location information."

Paragraphs [0107] – [0110] of *Liming* teach storing location information or context information in a cookie and then storing references to the cookies in the Client Position Table. The Client Position Table may include the system network address of the client with location contexts. In the example discussed in paragraphs [0107]-[0110], the location context information is stored in one or more cookies. However, nowhere does this passage teach or suggest the feature of "generating a unique name for an endpoint resource on the network device, wherein the unique name comprises the geographic location information."

Paragraphs [0160] – [0165] of *Liming* teach storing location information or context information in a Management Information Base and the advantages storing the information in this manner would be, such as easily allowing remote devices to access and alter the information. However, nowhere does this passage teach or suggest the feature of "generating a unique name for an endpoint resource on the network device, wherein the unique name comprises the geographic location information."

Thus, Appellants respectfully submit that *Liming* fails to teach or suggest the feature "generating a unique name for an endpoint resource on the network device, wherein the unique name comprises the geographic location information." Further *Hougaard* fails to cure the deficiencies of *Liming*. No portion of *Hougaard* teaches or suggests the feature of "generating a unique name for an endpoint resource on the network device, wherein the unique name comprises the geographic location information." *Hougaard* is silent regarding "generating a unique name for an endpoint resource on the network device, wherein the unique name comprises the geographic location information." Thus, the Final Office Action has fails to state a *prima facie* case of obviousness in regards to claims 4 and 21.

A.1.b Claims 5 and 22

Claims 5 and 22, which depend from claims 4 and 21, recite the feature of "associating the unique name with security attributes for the endpoint resource." The Final Office Action cites to *Hougaard*, column 7, line 1 to column 8, line 29 as allegedly teaching this feature. However, *Hougaard* fails to teach or suggest this feature.

As explained above, *Liming* in view of *Hougaard* fails to teach or suggest, "generating a unique name for an endpoint resource on the network device, wherein the unique name comprises the geographic location information." Therefore, logically, *Hougaard* cannot teach or suggest associating the unique name, which *Liming* in view of *Hougaard* failed to teach or suggest, with security attributes for the endpoint resource. Thus, *Hougaard* fails to teach or suggest the feature of "associating the unique name with security attributes for the endpoint resource." Thus, the Final Office Action has failed to state a *prima facie* case of obviousness in regards to claims 5 and 22, as the combination of *Liming* in view of *Hougaard* fails to teach or suggest the feature of "associating the unique name with security attributes for the endpoint resource."

A.1.c Claims 6 and 23

Claims 6 and 23, which depend from claims 4 and 21, recite the feature of "associating the unique name for the endpoint resource with the unique network hardware identifier." The Final Office Action cites to *Liming*, paragraphs 88-90, 107-110, and 156-165 as allegedly teaching this feature. However, *Liming* fails to teach or suggest this feature.

As explained above, *Liming* in view of *Hougaard* fails to teach or suggest, "generating a unique name for an endpoint resource on the network device, wherein the unique name comprises the geographic location information." Therefore, logically, *Liming* cannot teach or suggest associating the unique name, which *Liming* in view of *Hougaard* failed to teach or suggest, with "the unique network hardware identifier." Thus, *Liming* fails to teach or suggest the feature of "associating the unique name for the endpoint resource with the unique network hardware identifier." Thus, the Final Office Action has failed to state a *prima facie* case of obviousness in regards to claims 6 and 23, as the combination of *Liming* in view of *Hougaard* fails to teach or suggest the feature of "associating the unique name for the endpoint resource with the unique network hardware identifier."

A.1.d Claims 10 and 27

Claims 10 and 27 recite the feature of "detecting a change of location of the network device within the distributed data processing system based on the geographic location information." The Final

Office Action cites to paragraphs 91, 98-101, and 133 of *Liming* and to *Hougaard*, column 7, line 1 to column 8, line 29; column 8, line 53 to column 9, line 23 as allegedly teaching this feature. However, Appellants respectfully submit that these passages fail to teach or suggest the feature of "detecting a change of location of the network device within the distributed data processing system based on the geographic location information." Paragraph [0091] of *Liming* teaches the client can continuously send position information. Paragraphs [0098]-[0101] of *Liming* teach the client can send a continuous stream of location updates to a server and that the server stores the position data in a table. Paragraph [0133] of *Liming* teaches sending location relevant content to the device once the device's location and/or location context are known.

Nowhere do any of the cited passages of *Liming* teach or even suggest **detecting a change of location of the network device** within the distributed data processing system **based on the geographic location information**. Thus, *Liming* fails to teach or suggest the feature of "detecting a change of location of the network device within the distributed data processing system based on the geographic location information."

Column 7, line 1 to column 8, line 29 of *Hougaard* teaches creating and using context filters and access filters, which permits the user to receive geographic data that is relevant to the user, provided the user is authorized. However, as taught by *Hougaard*, the actual location of the user is not known or determined. Thus, a change in the location of the user is also not known or determined. Therefore, *Hougaard*, column 7, line 1 to column 8, line 29 fails to teach or suggest h the feature of "detecting a change of location of the network device within the distributed data processing system based on the geographic location information."

Column 8, line 53 to column 9, line 23 of *Hougaard* teaches that a user can interact with the geographic data and applications to generate a map and to alter the way it is presented based on user input. However, as taught by *Hougaard*, the actual location of the user is not known or determined. Thus, a change in the location of the user is also not known or determined. Therefore, *Hougaard*, column 8, line 53 to column 9, line 23 fails to teach or suggest the feature of "detecting a change of location of the network device within the distributed data processing system based on the geographic location information."

Thus, the Final Office Action has failed to state a *prima facie* case of obviousness in regards to claims 10 and 27, as the combination of *Liming* in view of *Hougaard* fails to teach or suggest the feature of "detecting a change of location of the network device within the distributed data processing system based on the geographic location information."

A.1.e Claims 11 and 28

Claims 11 and 28, which depend from claims 10 and 27, respectively, recite the feature of "reconfiguring the network device based on the detected change of location of the network device." The Final Office Action cites to paragraphs 91, 98-101, and 133 of *Liming* and to *Hougaard*, column7, line 1 to column 8, line 29; column 8, line 53 to column 9, line 23 as allegedly teaching this feature. Paragraph [0091] of *Liming* teaches that client can continuously send position information. Paragraphs [0098]-[0101] of *Liming* teach that client can send a continuous stream of location updates to a server and that the server stores the position data in a table. Paragraph [0133] of *Liming* teaches sending location relevant content to the device once the device's location and/or location context are known.

Nowhere do the any of the cited passages of *Liming* teach or even suggest, "reconfiguring the network device based on the detected change of location of the network device." Thus, *Liming* fails to teach or suggest the feature of "reconfiguring the network device based on the detected change of location of the network device."

Column 7, line 1 to column 8, line 29 of *Hougaard* teaches creating and using context filters and access filters, which permits the user to receive geographic data that is relevant to the user, provided the user is authorized. However, as taught by *Hougaard*, the actual location of the user is not known or determined. Thus, a change in the location of the user is also not known or determined. As *Hougaard* does not teach or suggest detecting a change in location of the network device, logically, *Hougaard*, column 7, line 1 to column 8, line 29 fails to teach or suggest h the feature of "reconfiguring the network device based on the detected change of location of the network device."

Column 8, line 53 to column 9, line 23 of *Hougaard* teaches that a user can interact with the geographic data and applications to generate a map and to alter the way it is presented based on user input. However, as taught by *Hougaard*, the actual location of the user is not known or determined. Thus, a change in the location of the user is also not known or determined. As *Hougaard* does not teach or suggest detecting a change in location of the network device, logically, *Hougaard*, column 8, line 53 to column 9, line 23 fails to teach or suggest h the feature of "reconfiguring the network device based on the detected change of location of the network device."

Thus, the Final Office Action has failed to state a *prima facie* case of obviousness in regards to claims 11 and 28, as the combination of *Liming* in view of *Hougaard* fails to teach or suggest the feature of "reconfiguring the network device based on the detected change of location of the network device."

A.1.f Claims 12 and 29

Claims 12 and 29, which depend from claims 10 and 27, respectively, recite the feature of "reconfiguring user security parameters based on the detected change of location of the network device." The Final Office Action cites to *Hougaard*, column7, line 1 to column 8, line 29; column 8, line 53 to column 9, line 23 as allegedly teaching this feature. However, *Hougaard* fails to teach or suggest this feature,

Column 7, line 1 to column 8, line 29 of *Hougaard* teaches creating and using context filters and access filters, which permits the user to receive geographic data that is relevant to the user, provided the user is authorized. However, as taught by *Hougaard*, the actual location of the user is not known or determined. Thus, a change in the location of the user is also not known or determined. As *Hougaard* does not teach or suggest detecting a change in location of the network device, logically, *Hougaard*, column 7, line 1 to column 8, line 29 fails to teach or suggest the feature of "reconfiguring user security parameters based on the detected change of location of the network device."

Column 8, line 53 to column 9, line 23 of *Hougaard* teaches that a user can interact with the geographic data and applications to generate a map and to alter the way it is presented based on user input. However, as taught by *Hougaard*, the actual location of the user is not known or determined. Thus, a change in the location of the user is also not known or determined. As *Hougaard* does not teach or suggest detecting a change in location of the network device, logically, *Hougaard*, column 8, line 53 to column 9, line 23 fails to teach or suggest the feature of "reconfiguring user security parameters based on the detected change of location of the network device."

Thus, the Final Office Action has failed to state a *prima facie* case of obviousness in regards to claims 11 and 28, as the combination of *Liming* in view of *Hougaard* fails to teach or suggest the feature of "reconfiguring user security parameters based on the detected change of location of the network device."

/Gerald H. Glanzman/
Gerald H. Glanzman
Reg. No. 25,035
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims involved in the appeal is as follows:

1. A method for management of a distributed data processing system, the method comprising:

determining a unique network hardware identifier for a network device;

associating the unique network hardware identifier with geographic location information; and

configuring the network device in accordance with the geographic location information through a network administrative user interface.

2. The method of claim 1 wherein the unique network hardware identifier is a MAC (Media Access Control) address.

3. The method of claim 1 further comprising:

authorizing user access to the network device based on a user security parameter corresponding to the geographic location information.

4. The method of claim 1 further comprising:

generating a unique name for an endpoint resource on the network device, wherein the unique name comprises the geographic location information.

5. The method of claim 4 further comprising:

associating the unique name with security attributes for the endpoint resource.

6. The method of claim 4 further comprising:

associating the unique name for the endpoint resource with the unique network hardware identifier.

7. The method of claim 4 further comprising:

determining a router closest to the endpoint resource;

retrieving router geographic location information associated with the router; and

using the router geographic location information in the generated unique name for the endpoint resource.

8. The method of claim 4 further comprising:

determining a network address generator (NAG) for the endpoint resource;

retrieving NAG geographic location information associated with the NAG; and

using the NAG geographic location information in the generated unique name for the endpoint resource.

9. The method of claim 8 wherein the network address generator is a server operating in accordance with a DHCP (Dynamic Host Configuration Protocol) protocol.

10. The method of claim 1 further comprising:

detecting a change of location of the network device within the distributed data processing system based on the geographic location information.

11. The method of claim 10 further comprising:

reconfiguring the network device based on the detected change of location of the network device.

12. The method of claim 10 further comprising:

reconfiguring user security parameters based on the detected change of location of the network device.

13. The method of claim 1 further comprising:

representing the distributed data processing system as a set of scopes, wherein a scope comprises a logical organization of network-related objects;

associating each scope with a management customer, wherein each scope is uniquely assigned to a management customer, wherein each scope is uniquely associated with a set of configuration parameters for managing each scope;

managing the distributed data processing system as a set of logical networks, wherein a logical network comprises a set of scopes, and wherein each logical network is uniquely assigned to a management customer; and

allowing an administrative user to dynamically reconfigure logical networks within the distributed data processing system.

14. The method of claim 1 further comprising:

dynamically discovering endpoints, systems, and networks within the distributed data processing system;

correspondingly representing endpoints, systems, and networks within the distributed data processing system as a set of endpoint objects, system objects, and network objects; and

logically organizing the endpoint objects, system objects, and network objects within a set of scopes, wherein each endpoint object, each system object, and each network object is uniquely assigned to a scope such that scopes do not logically overlap.

18. An apparatus for management of a distributed data processing system, the apparatus comprising:

means for determining a unique network hardware identifier for a network device;

means for associating the unique network hardware identifier with geographic location information; and

means for configuring the network device in accordance with the geographic location information through a network administrative user interface.

19. The apparatus of claim 18 wherein the unique network hardware identifier is a MAC (Media Access Control) address.

20. The apparatus of claim 18 further comprising:

means for authorizing user access to the network device based on a user security parameter corresponding to the geographic location information.

21. The apparatus of claim 18 further comprising:

means for generating a unique name for an endpoint resource on the network device, wherein the unique name comprises the geographic location information.

22. The apparatus of claim 21 further comprising:

means for associating the unique name with security attributes for the endpoint resource.

23. The apparatus of claim 21 further comprising:

means for associating the unique name for the endpoint resource with the unique network hardware identifier.

24. The apparatus of claim 21 further comprising:

means for determining a router closest to the endpoint resource;

means for retrieving router geographic location information associated with the router; and

means for using the router geographic location information in the generated unique name for the endpoint resource.

25. The apparatus of claim 21 further comprising:

means for determining a network address generator (NAG) for the endpoint resource;

means for retrieving NAG geographic location information associated with the NAG; and

means for using the NAG geographic location information in the generated unique name for the endpoint resource.

26. The apparatus of claim 25 wherein the network address generator is a server operating in accordance with a DHCP (Dynamic Host Configuration Protocol) protocol.

27. The apparatus of claim 18 further comprising:

means for detecting a change of location of the network device within the distributed data processing system based on the geographic location information.

28. The apparatus of claim 27 further comprising:

means for reconfiguring the network device based on the detected change of location of the network device.

29. The apparatus of claim 27 further comprising:

means for reconfiguring user security parameters based on the detected change of location of the network device.

30. The apparatus of claim 18 further comprising:

means for representing the distributed data processing system as a set of scopes, wherein a scope comprises a logical organization of network-related objects;

means for associating each scope with a management customer, wherein each scope is uniquely assigned to a management customer, wherein each scope is uniquely associated with a set of configuration parameters for managing each scope;

means for managing the distributed data processing system as a set of logical networks, wherein a logical network comprises a set of scopes, and wherein each logical network is uniquely assigned to a management customer; and

means for allowing an administrative user to dynamically reconfigure logical networks within the distributed data processing system.

31. The apparatus of claim 18 further comprising:

means for dynamically discovering endpoints, systems, and networks within the distributed data processing system;

means for correspondingly representing endpoints, systems, and networks within the distributed data processing system as a set of endpoint objects, system objects, and network objects; and

means for logically organizing the endpoint objects, system objects, and network objects within a set of scopes, wherein each endpoint object, each system object, and each network object is uniquely assigned to a scope such that scopes do not logically overlap.

35. A computer program product in a computer readable medium for use in managing a distributed data processing system, the computer program product comprising:

instructions for determining a unique network hardware identifier for a network device;

instructions for associating the unique network hardware identifier with geographic location information; and

instructions for configuring the network device in accordance with the geographic location information through a network administrative user interface.

36. The computer program product of claim 35 wherein the unique network hardware identifier is a MAC (Media Access Control) address.

37. The computer program product of claim 35 further comprising:

instructions for authorizing user access to the network device based on a user security parameter corresponding to the geographic location information.

EVIDENCE APPENDIX

This appeal brief presents no additional evidence.

RELATED PROCEEDINGS APPENDIX

This appeal has no related proceedings.